IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

UNITED STATES OF AMERICA	)	
	)	Case No. 3:24-cr-00151
v.	)	
	)	JUDGE RICHARDSON
MATTHEW ISAAC KNOOT	)	

RESPONSE OF THE UNITED STATES TO DEFENDANT'S MOTION TO SUPPRESS

Comes now the United States of America, by and through the undersigned Assistant United States Attorney, Joshua A. Kurtzman, and United States Department of Justice Trial Attorney Gregory J. Nicosia, Jr., and responds to the defendant's Motion to Suppress (hereinafter the "motion" or "motion to suppress"). (DE # 48.) The defendant's motion should be denied for at least four reasons. First, the Premises Warrant (DE # 48-1)[1] articulates adequate probable cause, particularity, and a nexus between the criminal conduct and the items to be seized. Moreover, Sixth Circuit precedent permits the seizure of all digital devices where, like here, the government is investigating crimes involving the pervasive use of digital devices. Second, the Discord Warrant (DE # 48-2) is appropriately tailored as it does not seek any and all information related to the account. The Discord Warrant sought only information that would identify the user of the account, devices used to access the account, times/locations when the account was accessed, and data related to the direct messaging feature that was being used to further the criminal conspiracy. Third, to the extent defendant seeks to challenge the information obtained from the Discord Warrant for his co-conspirator's account, the defendant lacks standing. Fourth, even assuming *arguendo* that the Court found these warrants to be defective, which it should not, the government

[1] Defendant's motion styles this warrant as a "Device Warrant," when, in reality, it is a premises warrant that authorized a search of defendant's residence, store unit, and the digital devices within those areas. (*See* DE # 48-1 at pg. 20.)

relied on the warrants in good faith. Good faith reliance on a defective search warrant should result in suppression "only in those unusual cases in which the exclusion will further the purposes of the exclusionary rule." *United States v. Leon*, 468 U.S. 897, 918 (1984). This case is not one of those unusual cases. Accordingly, the United States respectfully submits that the defendant's motion should be denied and a hearing on the defendant's motion is unnecessary.

PROCEDURAL BACKGROUND

On August 7, 2024, a Grand Jury in the Middle District of Tennessee indicted the defendant, charging him in Count One with Conspiracy to Damage Protected Computers, in violation of Title 18, United States Code, Section 371; Count Two with Conspiracy to Commit Money Laundering, in violation of Title 18, United States Code, Section 1956(h); Count Three with Conspiracy to Commit Wire Fraud, in violation of Title 18, United States Code, Section 1349; Count Four with Intentional Damage to a Protected Computer, in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (c)(4)(B), and (c)(4)(A)(i)(I); Count Five with Aggravated Identity Theft, in violation of Title 18, United States Code, Sections 1028(a)(1) and 2; and Count Six with Conspiracy to Cause the Unlawful Employment of Aliens, in violation of Title 18, United States Code, Section 371. (DE # 3.)

On October 4, 2024, the defendant filed an unopposed motion to continue trial, which was granted on November 7, 2024. (DE # 16 and 29.) On February 17, 2025, the defendant filed a second unopposed motion to continue trial, which was granted on February 18, 2025. (DE # 39 and 41.) Pursuant to the same order, Trial was scheduled for June 24, 2025. *Id*. On April 1, 2025, the defendant filed the instant motion to suppress. (DE # 48.)

FACTUAL BACKGROUND

The investigation of the defendant's criminal conduct began on April 4, 2023, when FBI Nashville received a complaint from a United States based company ("Victim 1") regarding suspicious online activity using a laptop computer provided by Victim 1 to an employee. (DE 48, Ex. A – Premises Warrant at ¶ 16.) Victim 1 shared with the FBI that its employee, A.M., had provided it with personally identifiable information, including a social security number and a home/mailing address in Nashville as part of the hiring/onboarding process. (*Id.* at ¶ 17.) Victim 1 reported that A.M., while working on the laptop that Victim 1 had mailed to the Nashville address, was connecting to a Chinese Internet Protocol ("IP") address through a Virtual Private Network (a "VPN"), which would be unnecessary and strange for his position at the company. (*Id.*) In the warrant, the case agent described that, "[a]s it relates to this application, publicly available VPNs can [] be used to proxy traffic across the Internet, to make Internet traffic appear as if is coming from another location." (*Id.* at ¶ 15.)

Victim 1 also reported that its company-issued laptop connected to its corporate network through a Wi-Fi network named "pretty fly for a wifi." (*Id.* at ¶ 22.)[2] The "pretty fly for a wifi" Wi-Fi network remained active as of on or about April 17, 2023 (before the search) and appeared to be emanating from 1818 Church Street, Apartment 103. *Id.* Thus, the FBI had at least two leads follow: (1) discovering the true identity of the employee hired as A.M. and using a Chinese IP address; and (2) determining who operated the computer network infrastructure, including the Wi-Fi network around Apartment 103, through which Victim 1's laptop connected to the Internet.

Based on the report from Victim 1, the FBI began investigating A.M.'s identity. Using the social security number provided by Victim 1, the case agent determined that A.M. was a resident

[2] In order to broadcast a Wi-Fi network to which a computer can connect, someone must set up a router, which is a device that connects computer networks or devices to the internet.

of Atlanta, Georgia, rather than Nashville, which, in part, led the case agent to believe that "violation[s] of 18 U.S.C. § 1030: Fraud and Related Activity in Connection with Computers; and 18 U.S.C. § 1028: Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information (the "Target Offenses") ha[d] been committed, are being committed, and/or will be committed by Matthew Knoot *and other persons as yet unknown*." (*Id.* at ¶ 7, 18.) (emphasis added). The FBI interviewed A.M. on June 14, 2023, and A.M. confirmed that he had never worked for Victim 1 and his identity had been stolen. (*Id.* at ¶ 18.)[3]

Armed with the knowledge that A.M.'s identity had been stolen and used to fraudulently obtain employment with a company that had issued the A.M. persona a laptop computer, the FBI conducted employment checks using various databases and identified several additional companies where A.M.'s personally identifiable information, including his social security number, were used to obtain remote work jobs. (*Id.* at ¶ 19.) Based on these results, FBI agents interviewed two additional companies ("Victim 2" and "Victim 3") that had hired an individual using A.M.'s personally identifiable information. Victim 2 and Victim 3, like Victim 1, confirmed that they each shipped company laptops to 1818 Church Street, Apartment 103, in Nashville, Tennessee after hiring an individual they believed was A.M. (*Id.* at ¶ 20.) Thus, at this juncture, computers from Victim 1, 2, and 3, were all sent and presumed present in Apartment 103.

The FBI confirmed that the defendant and a citizen of China, later determined to be the defendant's then girlfriend, were the sole occupants of the Apartment 103, based on information provided by the property management company for the 1818 Church Street apartment complex. (*Id.* at ¶ 21.) An FBI wireless survey also revealed that the "pretty fly for a wifi" wireless network, through which the Victim 1 laptop had connected to the corporate network, was active in the area

[3] Notably, both 18 U.S.C. §§ 1028 and 1030 make it a crime to attempt or conspire to commit any offense under sections 1028 and 1030. *See* 8 U.S.C. §§ 1028(f) and 1030(b).

around Apartment 103. FBI later learned that the defendant, with his then girlfriend, had relocated from Apartment 103 to Apartment 416 and was renting a storage unit (#2). (*Id.* ¶ 23.)[4]

In his affidavit, the case agent explained his basis of knowledge regarding cyber investigations and the items which he sought to seize and eventually search. The agent explained that "the majority of households and businesses in the United States now have access to personal computing device[s]" and "that records associated with illegal conduct are likely to be found on digital devices, including 'smartphones,'" which led him to request "permission to search all digital devices." (*Id.* at ¶ 24(a).) The case agent also stated that "believe[d] that one or more digital devices will be found during the search". (*Id.* ¶ 39.)

The case agent further explained that information stored on digital devices "can provide evidence of identity theft and identity of associates." (*Id.* at ¶ 24(b).) He believed he would find evidence related to the crimes under investigation because individuals who engage in identity theft and computer fraud:

- use digital devices to access websites to facilitate illegal activity;
- to communicate with co-conspirators online;
- to store documents and records relating to their illegal activity, which can include logs of online chats with coconspirators; email correspondence; text or other "Short Message Service" ("SMS") messages;
- to store contact information of co-conspirators, including telephone numbers, email addresses, identifiers for instant messaging and social medial accounts;
- to create and store media files such as photographs and video recordings; and

[4] As of the drafting of the Premises Warrant, the FBI had not yet determined the girlfriend's role in crimes under investigation, if any. At this time, the government has no reason to believe that the girlfriend participated in the charged conduct. This understanding only became apparent *after* execution of the Premises Warrant.

- to "back up" or transfer files from their old digital devices to that of their new digital devices, so as not to lose data, which would be valuable in facilitating their criminal activity.

(*Id.* at ¶ 26.)

The case agent continued by explaining that "[f]orensic evidence on a digital device can also indicate who has used or controlled the device" or "'*user attribution' evidence* [like] registry information, configuration files, user profiles, e-mail, e-mail address books, *chats*, *instant messaging logs*, photographs, the presence or absence of malware, *and correspondence* . . . [which] may be evidence of who used or controlled the digital device at a relevant time." (*Id.* at ¶ 27(b).) (emphasis added.)

Attachments A and B to the affidavit described the property to be searched and the items to be seized. The property to be searched was the defendant's apartment (Apartment 416), the storage area assigned to him, and "any digital devices within this residence or assigned storage area." (*Id.* Att. A.) The information, items, and data to be seized from the apartment, storage area, and digital devices were "fruits, evidence, information relating to, contraband, or instrumentalities, in whatever form and however stored, relating to violations of 18 U.S.C. § 1030: Fraud and Related Activity in Connection with Computers, 18 U.S.C. § 1028: Fraud and Related Activity in Connection with Identification Documents, Authentication Features." (*Id.* Att. B.) Such information, items, and data included, but was not limited to:

- *Business accounting records* to include customer information, contracts, ledgers, invoices, purchase orders, and payment records, *in whatever form*.
- Financial records, bank statements, deposit slips, money orders, monetary instruments, commercial receipts, and *other documents and materials reflecting financial activity* related to the Target Offenses.
- Cellular telephone(s), SIM cards, pre-paid calling cards, voice over IP (VOIP) communication devices and the accompanying bills, detailed call records, internet service contracts, e-mail account information, residential telephone account information and bills.

- *Electronic equipment, such as computers*, personal organizers, personal digital assistant (PDA), telex machines, facsimile machines, currency counting machines, pagers, telephone answering machines and related manuals used to generate, transfer, count, record and/or store information.

- Address and/or telephone books (written or typed by hand as opposed to printed commercially), including handwritten "owe sheets," rolodex indices *and any papers reflecting names, addresses, telephone numbers*, pager numbers, fax numbers and/or telex *numbers of co-conspirators*, sources of supply, customers, financial institutions and other individuals of businesses with whom a financial relationship exists, *and any financial records related to the alleged conspiracy*.

(*Id*.) (emphasis added.)

Attachment B to the warrant also specifically authorized "a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant." (*Id.*)

On August 2, 2023, Magistrate Judge Barbara D. Holmes approved the search warrant application that authorized the search of the defendant's apartment, storage unit, and digital devices therein. The FBI executed the warrant on August 8, 2023. (DE 49, Ex. B – Discord Warrant at ¶ 15.) Pursuant to the validly issued warrant, the FBI seized, among other things, a custom desktop computer belonging to the defendant. (*Id.*)

In a subsequent search of the computer seized from the defendant's apartment, the FBI discovered documents on the defendant's personal computer, which appeared to be saved Discord conversations between the defendant, using the moniker mellamomateo, and a co-conspirator, using the moniker yangdi0027, discussing their scheme to defraud. (Ex. B at pg. 12, ¶ 16.) This conversation discussed the address to which the victim computers were to be mailed to, the fees the defendant would receive for engaging in the computer fraud scheme, and other incriminating details of the criminal conspiracy. (*Id.*) Agents then served subpoenas to Discord confirming that the defendant's email address, matthewknoot@tutanota.com, was used to open the mellamomateo Discord account and confirming that the email address used to establish the yangdi0027 Discord

account belonged to defendant's co-conspirator. (*Id.* at ¶ 14-16.) On April 22, 2024, Magistrate Judge Holmes approved the search warrant application authorizing the search of the defendant and his co-conspirator's Discord accounts.

LEGAL ARGUMENT

The Fourth Amendment of the United States Constitution affords the right of individuals "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST., amend. IV. The Supreme Court has "expressed a strong preference for warrants," which "is most appropriately effectuated by according 'great deference' to a magistrate's determination." *United States v. Leon*, 468 U.S. 897, 913-14 (1984) (quoting S*pinelli v. United States*, 393 U.S. 410, 419 (1969)).

The task of a judicial officer evaluating an application for a search warrant is "to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the veracity and basis of knowledge of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983) (internal quotations omitted). In *Gates*, the U.S. Supreme Court reaffirmed the validity of the "totality-of-the-circumstances analysis that traditionally has informed probable cause determinations." *Id*. Here, "the duty of a reviewing court is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed." *Id*. at 238-39 (internal quotations and punctuation omitted).

In applying the probable cause standard, the Supreme Court has explained:

> Recital of some of the underlying circumstances in the affidavit is essential if the magistrate is to perform his detached function and not serve merely as a rubber stamp for the police. However, where these circumstances are

> detailed, where reason for crediting the source of the information is given, and when a magistrate has found probable cause, the courts should not invalidate the warrant by interpreting the affidavit in a hypertechnical, rather than a commonsense, manner. Although in a particular case it may not be easy to determine when an affidavit demonstrates the existence of probable cause, the resolution of doubtful or marginal cases in this area should be largely determined by the preference to be accorded to warrants.

United States v. Ventresca, 380 U.S. 102, 109 (1965); *see also Gates*, 462 U.S. at 236 ("[W]e have repeatedly said that after-the-fact scrutiny by courts of the sufficiency of an affidavit should not take the form of *de novo* review."). Finally, the Supreme Court has "recognized that affidavits are normally drafted by nonlawyers in the midst and haste of a criminal investigation. Technical requirements of elaborate specificity once exacted under common law pleading have no proper place in this area." *Ventresca*, 380 U.S. at 108.

1. The Premises Warrant Was Sufficiently Particularized.

As to the particularity of a warrant, a warrant "must enable the searcher to reasonably ascertain and identify the things which are authorized to be seized." *United States v. Savoy*, 280 F. App'x 504, 510 (6th Cr. 2008). The degree of detail "is flexible and will vary depending on the crime involved and the types of items sought." *United States v. Hanna*, 661 F.3d 271, 286 (6th Cir. 2011) (quoting *United States v. Greene*, 250 F.3d 471, 477 (6th Cir. 2001)); *see also Guest v. Leis*, 255 F.3d 325, 336 (6th Cir.2001) ("A search warrant must particularly describe the things to be seized, but the description, whose specificity will vary with the circumstances of the case, will be valid if it is as specific as the circumstances and the nature of the activity under investigation permit."). Moreover, a warrant need only be as specific as "the circumstances and the nature of the alleged crime permit," *United States v. Logan*, 250 F.3d 350, 365 (6th Cir. 2001), and as it relates to device warrants "a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable cause showing in the warrant application and affidavit demonstrate a

sufficient chance of finding some needles in the computer haystack." *United States v. Evers*, 669 F.3d 645, 653 (6th Cir. 2012). Indeed, the particularity requirement may even be satisfied through the express incorporation or cross-referencing of a supporting affidavit that describes the items to be seized, even though the search warrant contains no such description. *Baranski v. Fifteen Unknown Agents of Bureau of Alcohol, Tobacco & Firearms*, 452 F.3d 433, 439–40 (6th Cir. 2006).

"The cases on particularity are actually concerned with at least two rather different problems: one is whether the warrant supplies enough information to guide and control the agent's judgment in selecting what to take; and the other is whether the category as specified is too broad in the sense that it includes items that should not be seized." *United States v. Upham*, 168 F.3d 532, 535 (1st Cir.1999). It is the latter problem—overbreadth—that is alleged by the defendant in this case. "[I]nfirmity due to overbreadth does not doom the entire warrant; rather, it requires the suppression of evidence seized pursuant to that part of the warrant . . . but does not require the suppression of anything described in the valid portions of the warrant . . ." *Greene*, 250 F.3d at 477.

Courts that have addressed the appropriate breadth of computer-related searches have wrestled with how to balance two competing interests present in these searches:

> On one hand, it is clear that because criminals can—and often do—hide, mislabel, or manipulate files to conceal criminal activity, a broad, expansive search of the hard drive may be required.... On the other hand, ... granting the Government a carte blanche to search every file on the hard drive impermissibly transforms a limited search into a general one.

United States v. Stabile, 633 F.3d 219, 237 (3d Cir. 2011).

Despite the difficult nature of computer searches, the Sixth Circuit, along with the majority of other federal courts, have declined to demand the use of a specific search protocol and, instead, have employed the Fourth Amendment's bedrock principle of reasonableness on a case-by-case

basis: "While officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant, ... a computer search may be as extensive as reasonably required to locate the items described in the warrant based on probable cause." *United States v. Richards*, 659 F.3d 527, 538 (6th Cir. 2011) (citing *United States v. Burgess*, 576 F.3d 1078, 1092 (10th Cir. 2009)). The Sixth Circuit has expressed its agreement with the Tenth Circuit's succinct assessment in *Burgess* that:

> it is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives. One would not ordinarily expect a warrant to search filing cabinets for evidence of drug activity to prospectively restrict the search to "file cabinets in the basement" or to file folders labeled "Meth Lab" or "Customers." And there is no reason to so limit computer searches. But that is not to say methodology is irrelevant.
>
> A warrant may permit only the search of particularly described places and only particularly described things may be seized. As the description of such places and things becomes more general, the method by which the search is executed become[s] more important—the search method must be tailored to meet allowed ends. And those limits must be functional. For instance, unless specifically authorized by the warrant there would be little reason for officers searching for evidence of drug trafficking to look at tax returns (beyond verifying the folder labeled "2002 Tax Return" actually contains tax returns and not drug files or trophy pictures).
>
> Respect for legitimate rights to privacy in papers and effects requires an officer executing a search warrant to first look in the most obvious places and as it becomes necessary to progressively move from the obvious to the obscure. That is the purpose of a search protocol which structures the search by requiring an analysis of the file structure, next looking for suspicious file folders, then looking for files and types of files most likely to contain the objects of the search by doing keyword searches.
>
> But in the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders, and that is true whether the search is of computer files or physical files. It is particularly true with image files.

Id. at 539 (internal citations omitted).

Applying a reasonableness analysis on a case-by-case basis, the federal courts have rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers. *Richards*, 659 F.3d at 539 (citing *Guest*, 255 F.3d at 336) (rejecting particularity challenge to the seizure and off-site search of entire computers and their contents in an obscenity investigation because "the warrants required that the communications and computer records pertain to the listed offenses" and "[d]efendants could not have obtained more specific identification of e-mails and subscriber data, which were not accessible to them" and reasoning that "[a]lthough there were presumably communications on the computers that did not relate to the offenses, '[a] search does not become invalid merely because some items not covered by a warrant are seized.'"); *United States v. Henson*, 848 F.2d 1374, 1383 (6th Cir. 1988) (rejecting a Fourth Amendment challenge to the seizure of documents and computer files that were unrelated to the offenses because the Sixth Circuit concluded that it would have been unreasonable to require police to sort through extensive files in a suspect's office in order to separate out those items that were outside the warrant.); *Stabile*, 633 F.3d at 239 (determining that the search of a computer folder was objectively reasonable because "criminals can easily alter file names . . . to conceal contraband" and the officer "took steps to ensure that his investigation complied with the state search warrant"); *Upham*, 168 F.3d at 535 ("A sufficient chance of finding some needles in the computer haystack was established by the probable-cause showing in the warrant application; and a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs."). In other words, "[s]o long as the computer search is limited to a search for evidence explicitly authorized in the warrant, it is reasonable for the executing officers to open the various types of files located in the computer's hard drive in

order to determine whether they contain such evidence." *Richards*, 659 F.3d at 540. (citing *United States v. Roberts*, No. 3:08–CR–175, 2010 WL 234719, at *15 (E.D.Tenn. Jan. 14, 2010)).

The facts alleged in the Premises Warrant provided sufficient probable cause and particularity to authorize the search of the defendant's residence, storage unit, and digital devices therein. As articulated in *Evers,* there was absolutely probable cause in the warrant application and affidavit demonstrating a sufficient chance of finding some "needles in the computer haystack." The affidavit outlined that the defendant was engaged in a scheme to defraud using computers and A.M.'s stolen personally identifiable information, resulting in three victim companies shipping computers to the defendant's residence. While the warrant certainly permitted the seizure of the computers shipped by the victims to the defendant, the warrant articulated sufficient probable cause to believe that the defendant was using digital devices generally, including his personal phone and computer, to facilitate the fraud.

The affidavit particularly identifies that computer network infrastructure—the "pretty fly for a wifi" network—was set up within defendant's apartment. The affidavit further particularly identifies that Victim 1 reported that its company-issued laptop was accessed from that Wi-Fi network through a VPN from Chinese IP addresses. This, at minimum, indicated that one or more individuals located somewhere other than Nashville were accessing Victim 1's device. The warrant also particularly states that persons engaged in offenses under investigation use digital devices—and specifically their personal devices—to facilitate illegal activity and to communicate with their co-conspirators. Based on this information, it is a natural inference that the defendant needed to communicate with his non-Nashville-based co-conspirators and that he used his personal devices, rather than the victim companies' devices, to coordinate and facilitate the computer fraud scheme. The fact that the Victim 1 computer connected to its network from a VPN also suggests the

defendant and his conspirators were attempting obfuscate the true nature and location(s) of their activity because they had something to hide. It is likewise reasonable to conclude that the defendant and his co-conspirators took steps to keep their conversations private, including using their own devices, in order to avoid detection.

Regarding this point, defendant's motion incorrectly asserts that the Premises Warrant failed to indicate that more than one person was involved in the crimes under investigation. (DE # 48 at pg. 3, 13.) Indeed, the affidavit does not opine as to the number of potential co-conspirators, but it clearly articulates that at least two people occupied the defendant's residence, and, as just discussed, that someone located somewhere other than Nashville accessed Victim 1's device using sophisticated technical means. Defendant's motion also makes much of the fact that the case agent apparently "acknowledged that he didn't know whether the FBI would find any devices" in defendant's residence. (DE # 48 at pg. 3 and 9, fn.3.) This overly technical reading of ¶ 26 appears to fault the case agent for suggesting the possibility that the requested search warrant may not yield the evidence sought, which is belied by the fact that the search did yield probative evidence from defendant's computer. Moreover, this argument is foreclosed by the affidavit itself; the case agent stated that he "believe[d] that one or more digital devices will be found during the search". (Id. ¶ 39.)

There is good reason that in applying a reasonableness analysis on a case-by-case basis, federal courts have rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers. The search of defendant's residence for digital devices in this case was sufficiently particularized, and not overbroad, because evidence the crimes under investigation could have been found in any location on any of the digital devices present at the defendant's residence. As numerous courts have found, seizures, such as the one in this case,

are justified as long as evidence related to computer fraud could have been disguised or concealed somewhere on any of the digital devices. Likewise, the search and seizure conducted was not overbroad because a generalized seizure of digital devices is justified if it is demonstrated that the government could not reasonably segregate these devices on the basis of whether or not they were likely to evidence criminal activity. In cases involving digital evidence like this one, courts, including the Sixth Circuit, routinely reject claims that search warrants for all electronic devices at a premises were overbroad. *United States v. Evers*, 669 F.3d 645, 652–53 (6th Cir. 2012) ("The federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a 'sufficient chance of finding some needles in the computer haystack.'"); *see also United States v. Corleto*, 56 F.4th 169, 176-77 (1st Cir. 2022) (holding warrant for all electronic devices not overbroad in case involving online sharing of child pornography); *United States v. Adjani*, 452 F.3d 1140, 1146-47 (9th Cir. 2006) (same for online extortion, including computer belonging to another individual). Accordingly, the United States asserts that the Premises Warrant was sufficiently particularized.

Defendant's motion seems to argue that the Fourth Amendment's particularity requirement is heightened in searches of digital devices, owing in part to the array of personal information that can be stored on a digital device. (*See* DE # 48 at pg. 7-8.) No such requirement exists in the law. In support of this argument, defendant primarily relies upon two cases from other circuits: *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (finding that a warrant to search the defendant's computer was invalid for lack of particularity, and holding that the good faith exception to the exclusionary rule should apply) and *United States v. Griffith*, 867 F.3d 1265, 1275

(D.C. Cir. 2017). These cases are neither persuasive nor responsive to the specific facts at issue in this case.

Defendant first relies on *Otero* for the proposition that "warrants for [device] searches must affirmatively limit the search to the evidence of specific federal crimes or specific types of material," *Otero*, 563 F.3d at 1132. Here, Attachment B of the Premises Warrant was specifically limited to searches for information "relating to violations of 18 U.S.C. § 1030: Fraud and Related Activity in Connection with Computers, 18 U.S.C. § 1028: Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information, as described in the search warrant affidavit…". (Ex. A at pg. 21.) It is not a general warrant authorizing a search of *all* property for *any* evidence of crime. The mere fact that the warrant authorizes a search of all electronic devices—again for a limited category of information relating to the subject offenses—does not cause the warrant to be insufficiently particular.

Next, defendant relies on *Griffith* for the proposition that a device warrant must "specifically identify which devices are subject to search-and-seizure." *Griffith*, 867 F.3d at 1275-76. In *Griffith*, the warrant authorized a search for "all electronic devices to include but not limited to cellular telephone(s), computer(s), electronic tablet(s), devices capable of storing digital images . . .". *Id.* at 1276. This included searches of "any electronic device . . . even if police *knew* the device belonged to someone other than Griffith." *Id.* (emphasis original). However, the supporting affidavit offered no facts indicating that Griffith in fact owned a cell phone, or that any phone or other device containing incriminating information would be found in his apartment. *Id.* at 1268. *Griffith* is distinguishable for two reasons. First, the affidavit at issue in this case makes plain that at least three laptop computers were sent to defendant's home over a period of several months, and that someone within the defendant's residence operated computer network infrastructure that

enabled victim company devices to connect the Internet. Thus, it was reasonable for the FBI to request a warrant for any computers found within defendant's home because such computer(s) would almost certainly represent evidence or instrumentality of a crime. But indeed, the warrant sought was more limited than that; as noted above, the search was limited to "electronic equipment, such as computers…" for information "relating to violations of 18 U.S.C. § 1030: Fraud and Related Activity in Connection with Computers, 18 U.S.C. § 1028: Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information, as described in the search warrant affidavit…". (Ex. A at pg. 21.) Second, unlike in *Griffith*, the warrant here acknowledged that two people lived at the residence to be searched and that the residence could "contain storage media . . . predominantly used, and perhaps owned, by persons who are not suspected of a crime," and authorized the FBI to seize such devices *only* "[i]f it is nonetheless determined that . . . the things described in this warrant could be found on any of those computers or storage media." (Ex. A at ¶ 31.). Thus, the magistrate was aware of this fact and justified in issuing a warrant that authorized "a review of [all] electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant." (Id. at Att. B.) Accordingly, the Court should deny defendant's motion to dismiss.

2. The Premises Warrant Provided a Sufficient Nexus Between the Items Seized and the Alleged Criminal Conduct.

To support "a finding of probable cause, there must be a 'sufficient nexus' between the place searched and the evidence sought." *United States v. Kenny*, 505 F.3d 458, 461 (6th Cir. 2007) (citing *United States v. Carpenter*, 360 F.3d 591, 594 (6th Cir. 2004)). The Sixth Circuit, in line with numerous other circuits, has held, "whether a sufficient nexus has been shown to a particular location turns in part on the type of crime being investigated, the nature of the things to be seized,

the extent of an opportunity to conceal the evidence elsewhere, and the normal inferences that may be drawn as to likely hiding places." *United States v. Savoca*, 761 F.2d 292, 298 (6th Cir. 1985); *see also United States v. Carter*, 792 F. App'x 366, 369 (6th Cir. 2019) (citing *United States v. Castro*, 881 F.3d 961, 965 (6th Cir. 2018) ("[A] warrant that constrains a search to evidence of a specific crime satisfies the particularity requirement."); *United States v. Miggins*, 302 F.3d 384, 393-94 (6th Cir.), cert. denied, 537 U.S. 1130 (2002); *United States v. Gunter*, 551 F.3d 472, 481 (6th Cir.2009) ("[I]t was reasonable to infer that evidence of illegal activity would be found at Gunter's residence"); *Williams*, 544 F.3d at 688; *United States v. Stearn*, 597 F.3d 540, 554 (3d Cir.2010) ("Probable cause can be . . . inferred from the type of crime, the nature of the items sought, the suspect's opportunity for concealment, and normal inferences about where a criminal might hide [evidence]") (citation and quotation omitted); *United States v. Tate*, 586 F.3d 936, 943 (11th Cir.2009) ("Evidence that a defendant has stolen material which one normally would expect him to hide at his residence will support a search of his residence"); *United States v. Orozco*, 576 F.3d 745, 749 (7th Cir.2009) ("Warrants may be issued even in the absence of direct evidence linking criminal objects to a particular site"); *United States v. Ribeiro*, 397 F.3d 43, 49 (1st Cir. 2005) ("The probable-cause nexus . . . can be inferred from the type of crime, the nature of the items sought").

Probable cause does not require an actual showing of criminal activity at a particular location, but a "probability or substantial chance of criminal activity." *United States v. Davidson*, 936 F.2d 856, 859 (6th Cir. 1991); *see also United States v. Gann*, 732 F.2d 714, 722 (9th Cir.) cert. denied, 469 U.S. 1034 (1984). In *Abboud*, the defendant challenged an affiant's conclusions that relevant business and personal records would be found at his residence. The Sixth Circuit responded, "[o]ne does not need Supreme Court precedent to support the simple fact that records

of illegal business activity are usually kept at either a business location or at the defendant's home. Likewise, personal financial records are also usually stored at a person's home or place of business." *United States v. Abboud*, 438 F.3d 554, 572 (6th Cir. 2006). The *Abboud* court also held that the magistrate was justified in relying on the affiant's opinion about the location of the items to be seized as he was "a seasoned FBI special agent whose primary concentration [was] in financial crimes." *Id.* ("Defendant's claim that these were conclusory statements based on the affiant's "meager experience" misses the mark; the affiant is a seasoned FBI Special Agent whose primary concentration is in financial crimes. Certainly, his insight as to the probable location of the evidence of the crimes in this case cannot be denigrated as "pathetic averments," . . . Quite the contrary, the magistrate correctly relied on the affiant's experience in his assessment of the probable location of the evidence.").

In this case, the nexus between the place searched and the evidence sought is undeniable. As articulated in the Premises Warrant, at least three computers from victims of the defendant's computer fraud scheme were sent to his address. Legal process referenced in the affidavit also confirmed that those computers had been used in the defendant's residence and had connected to his wireless internet connection, which defendant, or another occupant of his home, would have had to set up. It is reasonable to infer that evidence related to computer fraud and identity theft would be found in the defendant's home and on his digital devices based on the nature of the crimes under investigation and the lack of any references in the affidavit to other physical locations (workplace, other residence, etc.) that the defendant frequented. In fact, there is nowhere else, other than the defendant's residence and on his digital devices, where it would be reasonable to infer that evidence related to identity theft and computer fraud would be found. Moreover, like in *Abboud,* the magistrate properly relied on the agent's specialized experience related to cybercrime

when the agent explained why he believed the evidence sought would be found in the place and devices to be searched.

Defendant's motion to suppress draws a distinction between victim company devices and defendant's personal devices, and then attacks the government's warrant as it relates to statements about defendant's personal devices as being mere boilerplate "training-and-experience" attestations. (*See* DE # 48 at pg. 9-11.) As it relates to the distinction between victim company devices and defendant's personal devices, the case agent's affidavit indicated that victim company devices were sent to defendant's home as part of scheme to defraud in violation of 18 U.S.C. §§ 1028 and 1030. Specifically, it describes how three laptops were sent to defendant's home after someone obtained employment with three separate companies under false pretenses—*i.e.*, the fraudulent use of A.M.'s identity—and that such devices were connected to computer network infrastructure within defendant's home. In investigating a crime in which computers are both an instrumentality of the offense and evidence of an offense itself, the distinction between a "victim" laptop and a "personal" laptop is unwarranted. Indeed, the Premises Warrant authorized the FBI to "locate not only electronic evidence or information that might serve as direct evidence of the crimes described in this statement, but also for forensic electronic evidence or information that establishes how the digital device(s) were used, the purpose of their use, who used them (or did not), and when." (*See* Ex. A at ¶27.)

Moreover, it was reasonable for the case agent to presume in an investigation concerning computer fraud, and for the limited purpose of articulating probable cause, that defendant used his personal devices in furtherance of the scheme whether that be for communication with conspirators, obfuscation of his identity, or to apply for new jobs. All of which are reasons set forth in the agent's affidavit. (*See* Ex. A at ¶ 26(a) (relating to communications), ¶¶15, 27(b), and

¶20 (relating to additional jobs procured in furtherance of the scheme.) Indeed, prior to obtaining the first laptop from Victim 1, defendant (or his co-conspirator(s)) somehow had to apply for or otherwise communicate with someone to get Victim 1 to ship a laptop to his home.

Despite the inclusion of this information in the affidavit, defendant's motion next argues that the nexus is insufficient because some of the case agent's assertions are made based on his training and experience, rather than specific facts gleaned through his investigation. (*See* DE # 48 at pg. 10-13.) Here, defendant relies principally on *United States v. Schultz*, 14 F.3d 1093, 1096 (6th Cir. 1994). It is true that *Schultz* held that an officer's training and experience "cannot substitute for the lack of evidentiary nexus" when determining probable cause. *Id.* at 1097-98; *but see Abboud*, 438 F.3d at 572. But *Schultz* is distinguishable on its facts. In *Schultz*, Officer Ideker arrested John Reid for selling a controlled substance. *Id.* at 1096. Reid told Ideker he purchased the drugs from James Leek, and that Leek's supplier owned an ice cream business around the corner from Leek's home. *Id.* Ideker then arrested Leek, who told Ideker that his local supplier was James Schultz and gave Ideker the phone number he had used to buy drugs. *Id.* Ideker's investigation revealed Schultz did in fact own the ice cream business; that Schultz had prior convictions for possession of marijuana products; and that Florida police had observed Schultz in Fort Myers, Florida. *Id.* Through a credit check, Ideker learned that Schultz maintained safe deposit boxes at the Ludlow Street branch of Star Bank in Cincinnati, and through a grand jury subpoena, Ideker identified the exact boxes. *Id.*

Based on this information, Ideker obtained a warrant to search Schutlz's safe deposit boxes at Star Bank, which the court later determined lacked probable cause. *Id.* at 1096, 1098. The Court held that Officer Ideker had not made any material connection between the bank and any criminal activity. *Id.* at 1097. The bank employees did not report any illegal activities related to the safe

deposit boxes, and Ideker had no other information connecting them to any illegal activity. *Id.* Instead, Ideker stated that "'[b]ased on his training and experience, [he] believe[d] ... that it is not uncommon for the records, etc. of such [drug] distribution to be maintained in bank safe deposit boxes.'" *Id*.

The warrant at issue in this case is distinguishable because it articulated a clear and specific nexus between the crimes under investigation and defendant's home. As noted above, the case agent's affidavit indicated that three laptops were sent to defendant's home as part of scheme to defraud in violation of 18 U.S.C. §§ 1028 and 1030 and that those laptops were subsequently connected to computer network infrastructure within defendant's home. From the outset, the government had demonstrated the existence of specific facts indicating that computers related to the offenses under investigation would be found in defendant's home. By contrast, in *Schultz* the warrant offered no nexus between the bank and any crime, let alone drug trafficking, whereas here defendant's home was the very scene of the crime as established by the case agent's affidavit. Thus, the case agent's additional assertions based on his training and experience about the defendant's personal devices were *in addition to* the previously proffered information establishing a clear nexus between electronic devices within defendant's home and the crimes under investigation, rather than the sole connection to such activity, as was the case in *Schultz*. Accordingly, *Schultz* should not be read as support for the instant motion to dismiss, and the Court should deny defendant's motion to dismiss.

Defendant makes two final attempts to persuade this Court that the Premises Warrant lacks a sufficient nexus to the crimes under investigation. First, he cites to four state decisions belaboring the claim that an officer's training and experience alone is insufficient to establish probable cause. (*See* DE # 48 at pg. 12.) While each case is individually distinguishable from the current matter, a

detailed discussion of each case is unnecessary. As argued above, the Premises Warrant does not rely solely on the case agent's training and experience, and there is a sufficient nexus between the Premises Warrant and the place to be searched. Here, the place to be searched was the defendant's residence for the evidence and instrumentalities of the offenses—the computers, corporate and personal—used to commit, further, and facilitate the scheme to defraud in violation of 18 U.S.C. §§ 1028 and 1030.

Second, defendant re-raises the arguments that: (1) the case agent apparently "acknowledged that he didn't know whether the FBI would find any devices" in defendant's residence, (DE # 48 at pg. 3 and 9, fn.3.); and (2) that the Premises Warrant failed to adduce any evidence of a conspiracy. (DE # 48 at pg. 3, 13.) Again, both arguments fall flat. As to the former, this overly technical reading of ¶ 26 that ignores the affiant's plain statement in ¶ 39 that he "believe[d] that one or more digital devices will be found during the search". (Id. ¶ 39.) As to the latter, there is ample evidence indicating that the defendant did not act alone. Specifically, at least two people occupied the defendant's residence, and someone located somewhere other than Nashville accessed Victim 1's device from a Chinese IP address.

3. The Discord Warrant Was Sufficiently Particularized.

As outlined above, the Premises Warrant established probable cause, was sufficiently particular about what was to be searched and seized, and adequately established a nexus between the alleged crimes and the items to be searched. As such, the evidence used from that search which provided probable cause for the search of the defendant's Discord account is not tainted. With that being the case, the defendant's sole remaining issue with the Discord Warrant is whether the warrant was sufficiently particular as it sought to seize data from the defendant's account.[5]

[5] Defendant's motion to dismiss appears to also argue that *all* information obtained from Discord—the information relating to defendant's account and his co-conspirator's account should be

As discussed above, the particularity requirement may be satisfied through the express incorporation or cross-referencing of a supporting affidavit that describes the items to be seized and "the degree of specificity required is flexible and will vary depending on the crime involved and the types of items sought." *Greene*, 250 F.3d at 477; *see also Guest*, 255 F.3d at 336 (6th Cir.2001) ("A search warrant must particularly describe the things to be seized, but the description, whose specificity will vary with the circumstances of the case, will be valid if it is as specific as the circumstances and the nature of the activity under investigation permit."). While there is no Sixth Circuit case explicitly addressing overbreadth in social media warrants, courts around the country have concluded that social media search warrants must be limited in scope. *See United States v. Allen*, 2018 WL 1726349, at *6 n. 25 (D. Kan. Apr. 10, 2018) (denying a motion to suppress for lack of particularity in a warrant seeking broad categories of Facebook account information because "the warrant was still limited to search for evidence relating to a specific crime, and it did not authorize on its face a search for every record associated with the Facebook accounts."); *United States v. Liburd*, 2018 WL 2709199 at *2 (E.D.N.Y. June 5, 2018) (Facebook search warrant was not overbroad because it was "limited by reference to an exemplary list of items to be seized ... related to the existence of ... [the] robbery conspiracy."); *United States v. Lowry*, 2015 WL 4399627 at *3 (S.D. Ohio July 17, 2015) (search warrant for "all communications between any user or recipient and the substance of those communications" was not overbroad where Defendant used Facebook Messenger to exchange nude photographs with minors.).

Here, despite the defendant's arguments to the contrary, the Discord Warrant was sufficiently particular and did not seek access to all data associated with the account. Instead, the Discord Warrant sought a discrete categories of data based on records of saved chats between the

---

suppressed. (*See* DE # 48 at pg. 15.) For the reasons discussed *infra*, Defendant lacks standing to challenge the Discord returns as they relate to his co-conspirator's account.

defendant and an unindicted co-conspirator. The warrant sought two general types of data: (1) data that could be used to identify the user of the Discord account; and (2) data associated with the criminal activity under investigation. With respect to the identity data sought, Attachment B of the Discord Warrant, subparagraphs a – g, all seek information, like full name, email address, physical address, date of birth, gender, hometown, occupation, Internet Protocol information, and other data that would allow the government to determine the identity of the user of the account, identify the devices used to access the account, and determine from when and where the account was accessed. All that information would aid the government in identifying the user of the Discord account in question and probable cause existed for the government to seek this data based on the probable cause statement contained in the affidavit in support of the search warrant. Likewise, the portions of the Discord Warrant seeking any messages to or from the defendant's Discord account is similarly tailored based on the evidence that the defendant was using his Discord account to engage in the criminal conduct under investigation. The tailoring of the warrant here to data that would reveal the user of the Discord account and the messaging portion of the account that the government knew was being used to further the criminal conspiracy distinguishes this warrant entirely from the one at issue in the case cited by the defendant, *United States v. Mercery*, 591 F. Supp. 3d 1369, 1381 (M.D. Ga. 2022). *Mercery*, upon which the defendant relies, authorized the seizure of all data associated with a social media account, which is not at all what occurred here. Accordingly, the Court should deny the defendant's motion to suppress as it pertains to the Discord Warrant.

4. Defendant Lacks Standing to Challenge the Discord Warrant for his Co-Conspirator's Account.

Notwithstanding the fact the Discord Warrant is valid and should not be suppressed, the defendant also lacks standing to challenge the Discord Warrant for his co-conspirator's account.

The protection offered by the Fourth Amendment is personal, and only a victim of an unconstitutional search and seizure has standing to challenge the search. *See Plumhoff v. Rickard*, 572 U.S. 765 (2014); *Brown v. United States*, 411 U.S. 223 (1973); *Alderman v. United States*, 394 U.S. 165 (1969). Furthermore, a person who is not a victim of an unconstitutional search and seizure cannot object to the introduction of the evidence seized, and federal court are not authorized to suppress otherwise admissible evidence on the ground that it was unlawfully seized from a third party who is not before the court. *Goldstein v. United States*, 316 U.S. 114 (1942); *United States v. Payner*, 447 U.S. 727 (1980). As a general rule, a person who brings a motion to suppress evidence on the ground that it was seized during an illegal search must assert an interest in the property seized, or possessory interest in the premises searched. *Rakas v. Illinois*, 439 U.S. 128 (1978). Here, it is defendant's co-conspirator Yang Di, not defendant, that has a possessory interest in the yandi0027 account, which was authorized to be searched by the Discord Warrant. Thus, defendant cannot complain to this Court that the Discord Warrant is constitutionally infirm with respect to the evidence obtained about the yandi0027 account. Accordingly, the Court should, at a minimum, deny the defendant's motion to suppress as it pertains to the Discord Warrant returns for the yandi0027 account.

5. The *Leon* Good Faith Exception Applies Even if the Court Deemed Either of the Warrants Constitutionally Deficient.

Even if the two search warrants in this case were defective, which they are not, the defendant's motion to suppress still fails under the *Leon* good-faith exception. As the Sixth Circuit has noted, even if a search warrant is defective, courts will not suppress evidence seized pursuant to such warrant if the seizure was based on reasonable, good faith reliance on the warrant. *United States v. Frazier*, 423 F.3d 526, 533 (6th Cir.2005) (citing *United States v. Leon*, 468 U.S. 897, 905 (1984)). The Supreme Court explained the mechanics of the good faith exception:

> [O]ur good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization. In making this determination, all of the circumstances—including whether the warrant application had previously been rejected by a different magistrate—may be considered.

Leon, 468 U.S. at 922–23 n. 23.

The rationale behind the exception is that the exclusionary rule is meant to deter unlawful police conduct. *Abboud*, 438 F.3d at 578. This policy of deterrence is not served by the exclusion of evidence seized in good faith by the police. *Id.* (citing *Leon*, 468 U.S. at 918–19). The only instances where the good faith exception does not apply are in the following specific circumstances: "1) the supporting affidavit contained knowing or reckless falsity; 2) the issuing magistrate wholly abandoned his or her judicial role; 3) the affidavit is 'so lacking in probable cause as to render official belief in its existence entirely unreasonable;' or 4) where the officer's reliance on the warrant was neither in good faith nor objectively reasonable." *Frazier*, 423 F.3d at 533 (quoting *Leon*, 468 U.S. at 923).

In *Evers,* after finding that the warrant was sufficiently particular, the Sixth Circuit noted that even if it was not, the motion to suppress would be properly denied under the good faith exception. *United States v. Evers*, 669 F.3d 645, 654 (6th Cir. 2012). The Sixth Circuit noted that the search warrant cross referenced the agent's affidavit which "recited the underlying factual circumstances of the alleged [] crimes, identified the victim, gave the address of [the defendant's] residence, and listed" a plethora of digital devices that were objects subject to seizure. *Id.* The Sixth Circuit then concluded that the law enforcement officers involved in the search and seizure of the digital devices properly relied on the warrant signed by the magistrate. *Id.*

While the Court should find both the Premises and Discord Warrants constitutionally valid, if it does not, Court should deny the defendant's motion to suppress based on the good faith

exception. Both warrants in this case outline a sufficient factual basis to establish that probable cause existed to believe that computer fraud and identity theft crimes occurred, the defendant was involved, the defendant had computers and devices associated with the fraud scheme at his residence, and the defendant used his Discord account to further the criminal conspiracy. Moreover, the defendant does not cite any Sixth Circuit case that would put the government on notice that its reliance on either of these two warrants was impermissible. With respect to the Premises Warrant, the defendant ignores Sixth Circuit cases that dictate that the warrant is permissible and relies on distinguishable state decisions. Likewise, with respect to the Discord Warrant, the defendant relies on a district court decision from another circuit that is completely distinguishable. Finally, defendant's motion to suppress does not address the good faith exception to the warrant requirement at all, nor does it allege that any of the factors outlined in *Frazier* apply to the instant case. 423 F.3d at 533 (quoting *Leon*, 468 U.S. at 923). As such, even if the Court were to take issue with either of these warrants, which it should not, it should still find that the government acted in good faith reliance on the warrants which were both approved by the magistrate. Accordingly, the defendant's motion to suppress should be denied in its entirety.

CONCLUSION

Based on the foregoing, the United States respectfully submits that the Court should deny the defendant's Motion to Suppress and do so without an evidentiary hearing.

Respectfully submitted,

ROBERT E. MCGUIRE
Acting United States Attorney

By: *s/ Joshua A. Kurtzman*

JOSHUA A. KURTZMAN
Assistant U. S. Attorney
719 Church Street - Suite 3300
Nashville, Tennessee 37203-3870
Telephone: 615-401-6617

s/ Gregory Jon Nicosia, Jr.
GREGORY JON NICOSIA, JR.
D.C. Bar No. 1033923
Trial Attorney
National Security Division
950 Pennsylvania Avenue, NW
Washington, DC 20530
(202) 353-4273
Gregory.Nicosia@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that the above document was filed through the ECF system and will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF).

Date: April 14, 2025

/s/ Joshua A. Kurtzman
JOSHUA A. KURTZMAN
Assistant United States Attorney
Middle District of Tennessee